(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2005 (02.06.2005)

PCT

(10) International Publication Number
WO 2005/050908 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number:
PCT/EP2004/012226

(22) International Filing Date: 28 October 2004 (28.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0325225.1 29 October 2003 (29.10.2003) GB
0401470.0 23 January 2004 (23.01.2004) GB

(71) Applicant *(for all designated States except US)*: **ARGEL-COM LIMITED** [GB/GB]; Osborne Clarke, 2 Temple Back East, Temple Quay, Bristol BS1 6EG (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SMART, Nigel, Paul** [GB/GB]; 6 Prowse Close, Thornbury, Bristol BS35 1EG (GB).

(74) Agent: **McGOWAN, Nigel, George**; Intellectual Property Department, Siemens Shared Services, Siemens House, Oldbury, Bracknell, Berkshire, RG12 8FZ (US).

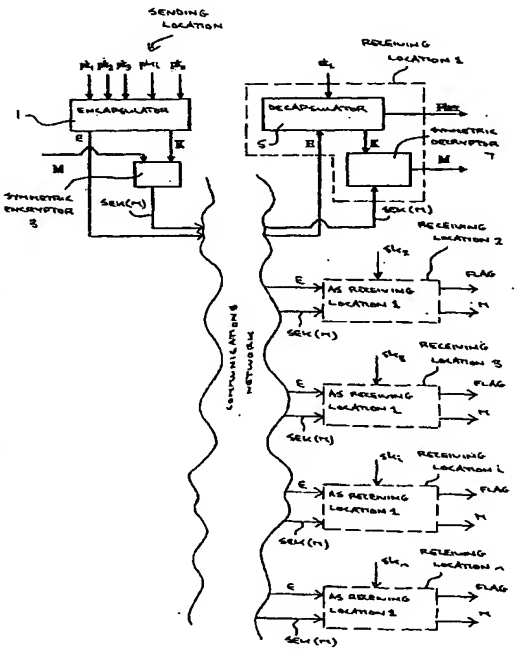
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A SECURE CRYPTOGRAPHIC COMMUNICATION SYSTEM USING KEM-DEM



(57) **Abstract:** A secure communication system comprising: a communications network; at a sending location on said network: (i) an encapsulator (1) for providing (a) a session key (K), and (b) plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)), each said encryption corresponding to a respective receiving location (1 to n) on said network; and (ii) a symmetric encryptor (3) for utilising said session key (K) to encrypt a message (M); and, at each said receiving location (1 to n) on said network: (i) a decapsulator (5) for decrypting the encryption of said plurality of encryptions (E1(K), E2(K), E3(K) ... Ei(K) ... En(K)) which corresponds to that receiving location (1 to n) to provide said session key (K); and (ii) a symmetric decryptor (7) for utilising the session key (K) to decrypt the message (M), said encapsulator (1) comprising: a pseudo random number generator (51 or 91); symmetric key derivation means (55 or 95) for deriving said session key (K) from a first random number (N) generated by said pseudo random number generator (51 or 91); means (53 or 93) for utilising said first random number (N) to generate a second random number (r); and means (57-0 to 57-n and 59-1 to 59-n, or 97-1 to 97-n and 99-1 to 99-(n-1) and 101-(-1) to 101-(n-1) and 103 and 105 and 107) for utilising the first keys (pk1 to pkn, or id1 to idn) of asymmetric encryption key pairs (pk1 to pkn and sk1 to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) together with said second random number (r) and said first random number N to generate said plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3 (K) ... Ei(K) ... En(K)), said decapsulator (5) at each receiving location (1 to n) comprising: means (71, 73, 75, or 111, 113, 115 or 131, 133, 135, 137, 139, 141) for utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the recipient at the receiving location together with the asymmetric encryption (Ei(K)) corresponding to the receiving location to recover said first random number (N); and a further symmetric key derivation means (77, or 117 or 143) for deriving said session key (K) from said first random number (N).

WO 2005/050908 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.